## AMENDMENTS TO THE CLAIMS

This Listing of Claims will replace all prior versions and listings of claims in this application.

Listing of Claims:

1. (Currently amended) A method of secure data exchange between a master cryptographic unit and a slave cryptographic unit, comprising the steps of:

sending either a reset message or a key validation message to request the master cryptographic unit to validate a key held by the slave cryptographic unit during each session; and

forwarding a key exchange message, which includes a new key encrypted through the key held by the slave cryptographic unit, from the master cryptographic unit to the slave cryptographic unit.

2. (Original) The method of secure data exchange of claim 1, further comprising a step of sending a key confirmation message to notify the master cryptographic unit that the new key is correctly received by the slave cryptographic unit.

3. (Currently amended) The method of secure data exchange of claim 2, further comprising the steps of:

responding to the key confirmation message with a downloading message to allow the slave cryptographic unit ~~retrieving~~ to retrieve requested information; and

sending a finish message to the master cryptographic unit after the requested information is completely downloaded.

4. (Original) The method of secure data exchange of claim 1, wherein the reset message requests the master cryptographic unit to validate an initial key held by the slave cryptographic unit.

5. (Original) The method of secure data exchange of claim 4, wherein the initial key is either pre-configured by factories and permanently stored in the slave cryptographic unit or obtained from the master cryptographic unit through a manual login.

6. (Original) The method of secure data exchange of claim 1, further comprising a step of notifying the slave cryptographic unit that the key is invalid after the key validation message is sent.

7. (Currently amended) The method of secure data exchange of claim 6, further comprising a step of sending the ~~rest~~ reset message to request the master cryptographic unit to validate an initial key held by the slave cryptographic unit.

8. (Original) The method of secure data exchange of claim 3, further comprising the steps of:

sending another key validation message to request the master cryptographic unit to validate the new key held by the slave cryptographic unit; and

forwarding another key exchange message, which includes a renewed key encrypted through the new key held by the slave cryptographic unit.

9. (Currently amended) The method of secure data exchange of claim 1, further comprising a step of notifying the slave cryptographic unit that the key is invalid after the ~~resent~~ reset message is sent.

10. (Original) The method of secure data exchange of claim 1, wherein the master cryptographic unit is a key distribution server.

11. (Original) The method of secure data exchange of claim 10, wherein the key distribution server is included in an automatic provisioning system.

12. (Original) The method of secure data exchange of claim 10, wherein the slave cryptographic unit is a client.

13. (Original) The method of secure data exchange of claim 10, wherein the reset message includes an initial key, a physical address of the slave cryptographic unit, timestamp data and hash data.

14. (Original) The method of secure data exchange of claim 10, wherein the key validation message includes the key, a physical address of the slave cryptographic unit, timestamp data and hash data.